THE MILBANK QUARTERLY
A MULTIDISCIPLINARY JOURNAL OF POPULATION HEALTH AND HEALTH POLICY

Op-Ed

Data Withholding in the Age of Digital Health

DAVID BLUMENTHAL

Every technological advance brings both benefits and risks, many of which are unanticipated. This is especially true of digitizing health information—a process that is inevitable and accelerating. Since the dawn of the information revolution, the very idea that health care would remain walled off from this profound development has been untenable. The question was not if but when, and with what effects. For example, the so-called 21st Century Cures Act has numerous unheralded provisions that clearly indicate bipartisan support for health information exchange (HIE) and bipartisan impatience with the failure of vendors and providers to facilitate it.[1]

It is important to recognize that these effects are not fixed but evolving. The benefits and risks of digitized health information will change as health information technologies advance and as professionals and patients become more familiar with them. An important example of how effects may evolve is the concern about patients withholding data. The worry is that patients may be reluctant to share sensitive information with clinicians in the digital age for fear that their data will be insecure, which is not unrealistic, given almost daily reports of hacking into supposedly protected databases.

Such fears are likely to grow as HIE becomes widespread. HIE consists of a largely unrealized capability to move individuals' health information around the health system for clinical, administrative, and investigational purposes. This raises the prospect that sensitive data may be both *routinely* and *intentionally* shared in ways that patients find concerning. More troubling, data on the move may be inherently less secure than data stored behind institutional firewalls.

The withholding of data by patients creates many problems.[2] It reduces the accuracy and completeness of the information available to the health care professionals responsible for making diagnostic and therapeutic decisions. From the patients' standpoint, this may

The Milbank Quarterly, Vol. 95, No. 1, 2017 (pp. 15-18)

compromise the quality of care they receive. From the clinicians' standpoint, data withholding may increase the frustration and risks of clinical practice. Clinicians take pride in their profession and are demoralized when missing information compromises their skills. Health professionals may also fear being held legally liable for failing to elicit information that patients are reluctant to provide.

That said, HIE brings huge potential benefits for patients, clinicians, and society. HIE facilitates better and safer care for patients.[3] It may reduce society's health care expenses—and patients' out-of-pocket costs—by avoiding unnecessary diagnostic and therapeutic interventions. The sharing of accurate and complete data encourages clinicians to practice at the top of their game. It may also facilitate cutting-edge research by means of accessing and analyzing patient data repositories created through HIE.

As we grapple with the growing concerns over data withholding, the first task is to make sure these concerns are real. Research is required to document the nature and extent of patients' failure to share health information: to understand who withholds data, what they withhold, and how often they do so. The epidemiology of the phenomenon may suggest important ways to minimize it.

Minimizing the risks of new technologies is a logical first step toward optimizing their value. Assuming for the moment that data withholding will occur—as it has long occurred in the world of paper medical records as well—a number of strategies could reduce the frequency and the downside of patients' withholding of health information.

All these strategies, in my view, should be consistent with one overarching premise: patients own and should control their health care data and have no obligation to share information that they prefer to withhold.

Donald Berwick eloquently described the bedrock principle of patient autonomy: We (clinicians) are all "guests in their lives," and we need to live by the rules of the house.[4]

Some clinicians may seek to prevent data withholding by threatening not to care for patients who do so. But this approach violates the fundamental requirement that health professionals put patients' interests—real or perceived—ahead of their own. Clinicians are trained to function without perfect information. Patient data withholding is just one more contributor to the challenging information reality that health professionals have faced while gathering their patients' medical histories since, at least, the age of Hippocrates. (There are, of course, circumstances when

patients' data withholding can affect the welfare of others, for example, when they are carrying or are exposed to a communicable disease. In such cases, patients' rights to data withholding may be circumscribed.)

Clinicians, health care organizations, and vendors can and should reduce the frequency of patient data withholding. First, they should create the most secure possible environment for the data health professionals collect. In fact, the most common reason for highly publicized data breaches in health care is not malicious hacking, but health care providers' bad data hygiene.[5] Many health professionals and organizations do not observe the most basic security precautions, such as requiring and training their employees to observe basic security procedures.

Second, they should educate patients on the benefits and risks of data sharing and withholding so that they can make informed decisions. With appropriate education, patients can give meaningful consent (or nonconsent) to providers' participation in data sharing on their patients' behalf.

Finally, technological innovation designed to increase patients' ability to exert granular control over their health information may constitute a third way of minimizing data withholding. If patient portals and other devices through which patients access their health information can offer them choices on what they are willing to share, and with whom, they may feel more confident in the integrity of the data systems that store their health information.

In the near future, electronic means of gathering and storing patient data will become normative. In the meantime, we will have to manage the problems that come with the territory. The key is to recognize patients' unquestioned right to control their health care fate, including their health information, and to minimize the risks of data sharing, maximize the benefits, and make it technologically safe and easy to participate.

References

1. Pitman D. Cures goes to vote. *Politico*. November 30, 2016. http://www.politico.com/tipsheets/morning-ehealth/2016/11/cures-goes-to-vote-217631. Accessed December 5, 2016.
2. Caine K, Tierney WM. Point and counterpoint: patient control of access to data in their electronic health records. *J Gen Intern Med*. 2015;30(Suppl. 1):38-41.

3. Vest JR, Kern LM, Silver MD, Kaushal R; HITEC investigators. The potential for community-based health information exchange systems to reduce hospital readmissions. *J Am Med Inform Assoc*. 2015;22(2):435-442.
4. Berwick DM. What "patient-centered" should mean: confessions of an extremist. *Health Aff.* (Millwood). 2009;28(4):w555-w565.
5. Blumenthal D, McGraw D. Keeping personal health information safe: the importance of good data hygiene. *JAMA*. 2015;313(14):1424.

Address correspondence to: David Blumenthal, MD, The Commonwealth Fund, 1 E 75th St, New York, NY 10021 (email: db@cmwf.org).